I

(Entschließungen, Empfehlungen und Stellungnahmen)

STELLUNGNAHMEN

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE

Stellungnahme des Europäischen Datenschutzbeauftragten zum Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung unter anderem der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Richtlinie über den Schutz der Privatsphäre und elektronische Kommunikation)

(2008/C 181/01)

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE —

gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft, insbesondere auf Artikel 286,

gestützt auf die Charta der Grundrechte der Europäischen Union, insbesondere auf Artikel 8,

gestützt auf die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ([1]),

gestützt auf die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation ([2]),

gestützt auf die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr ([3]), insbesondere auf Artikel 41,

gestützt auf das am 16. November 2007 eingegangene Ersuchen der Europäischen Kommission um Stellungnahme nach Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 —

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

I. EINLEITUNG

1. Die Kommission hat am 13. November 2007 einen Vorschlag für eine Richtlinie zur Änderung unter anderem der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (nachstehend „Vorschlag“ oder „vorgeschlagene Änderungen“ genannt) angenommen. Die gegenwärtige Fassung der Richtlinie 2002/58/EG wird üblicherweise, so auch in dieser Stellungnahme, als Datenschutzrichtlinie für die elektronische Kommunikation bezeichnet.

([1]) ABl. L 281 vom 23.11.1995, S. 31.
([2]) ABl. L 201 vom 31.7.2002, S. 37.
([3]) ABl. L 8 vom 12.1.2001, S. 1.

2. Mit dem Vorschlag wird darauf abgezielt, den Schutz der Privatsphäre und der personenbezogenen Daten der Bürger bei der elektronischen Kommunikation zu verbessern. Dies erfolgt nicht durch eine vollkommene Umgestaltung der geltenden Datenschutzrichtlinie für die elektronische Kommunikation, sondern dadurch, dass Ad-hoc-Änderungen vorgeschlagen werden, die in erster Linie darauf abzielen, dass die sicherheitsbezogenen Bestimmungen gestärkt und die Durchsetzungsmechanismen verbessert werden.

3. Der Vorschlag ist Teil einer umfassenderen Reform der fünf Telekommunikations-Richtlinien der EU („Telekommunikations-Paket"). Zusätzlich zu den Vorschlägen für die Überprüfung des Telekommunikations-Pakets ([1]) hat die Kommission zur gleichen Zeit einen Vorschlag für eine Verordnung zur Einrichtung der Europäischen Behörde für die Märkte der elektronischen Kommunikation ([2]) angenommen.

4. Die in dieser Stellungnahme enthaltenen Bemerkungen beschränken sich auf die vorgeschlagenen Änderungen an der Datenschutzrichtlinie für die elektronische Kommunikation, außer wenn sich die vorgeschlagenen Änderungen auf Begriffe oder Bestimmungen stützen, die in Vorschlägen für die Überprüfung des Telekommunikations-Pakets enthalten sind. Darüber hinaus beziehen sich einige Bemerkungen in dieser Stellungnahme auf Bestimmungen der Datenschutzrichtlinie für die elektronische Kommunikation, die durch den Vorschlag nicht geändert werden.

5. In dieser Stellungnahme werden die folgenden Themen behandelt: i) der Anwendungsbereich der Datenschutzrichtlinie für die elektronische Kommunikation, insbesondere die betroffenen Dienste (vorgeschlagene Änderung an Artikel 3 Absatz 1); ii) die Benachrichtigung über Sicherheitsverletzungen (vorgeschlagene Änderung, durch die Artikel 4 Absätze 3 und 4 geschaffen wird); iii) die Bestimmungen über Cookies, Spyware und ähnliche Instrumente (vorgeschlagene Änderung an Artikel 5 Absatz 3); iv) das gerichtliche Vorgehen von Anbietern elektronischer Kommunikationsdienste und anderer juristischer Personen (vorgeschlagene Änderung, mit der Artikel 13 Absatz 6 geschaffen wird) und v) die Stärkung der Bestimmungen über die Umsetzung und Durchsetzung (vorgeschlagene Änderung, mit der Artikel 15a geschaffen wird).

Konsultierung des EDSB und der Öffentlichkeit

6. Die Kommission hat den Vorschlag am 16. November 2007 dem EDSB übermittelt. Der EDSB versteht diese Übermittlung als Ersuchen um Beratung von Organen und Einrichtungen der Gemeinschaft nach Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr (nachstehend „Verordnung (EG) Nr. 45/2001" genannt).

7. Die Kommission hat den EDSB vor der Annahme des Vorschlags informell zum Vorschlagsentwurf konsultiert; der EDSB hat dies begrüßt, da er dadurch Gelegenheit hatte, vor der Annahme des Vorschlags durch die Kommission einige Vorschläge zum Vorschlagsentwurf zu machen. Der EDSB ist erfreut, dass sich einige seiner Anregungen in dem Vorschlag widerspiegeln.

8. Der Annahme des Vorschlags ging eine Konsultierung der Öffentlichkeit voraus, eine Praxis, die der EDSB begrüßt. Die Kommission hatte im Juni 2006 eine Konsultierung der Öffentlichkeit zu ihrer Mitteilung zur Überprüfung des Telekommunikations-Pakets eingeleitet, in der die Kommission ihre Standpunkte zur Sachlage beschrieben und einige Änderungsvorschläge unterbreitet hat ([3]). Die Datenschutzgruppe „Artikel 29", der der EDSB angehört, hat diese Gelegenheit genutzt, um ihre Standpunkte zu den vorgeschlagenen Änderungen in einer Stellungnahme darzulegen, die am 26. September 2006 angenommen wurde ([4]).

([1]) Die vorgeschlagenen Änderungen an den Telekommunikations-Richtlinien sind in den folgenden Vorschlägen enthalten: i) Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinie 2002/21/EG über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste, der Richtlinie 2002/19/EG über den Zugang zu elektronischen Kommunikationsnetzen und zugehörigen Einrichtungen sowie deren Zusammenschaltung und der Richtlinie 2002/20/EG über die Genehmigung elektronischer Kommunikationsnetze und -dienste, 13. November 2007, KOM(2007) 697 endg.; ii) Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, 13. November 2007, KOM(2007) 698 endg.

([2]) Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Einrichtung der Europäischen Behörde für die Märkte der elektronischen Kommunikation, 13. November 2007, KOM(2007) 699 endg.

([3]) Mitteilung über die Überprüfung des EU-Rechtsrahmens für elektronische Kommunikationsnetze und -dienste (SEK(2006) 816), die am 29. Juni 2006 angenommen wurde. Die Mitteilung ist durch ein Arbeitspapier der Kommissionsdienststellen ergänzt worden (KOM(2006) 334 endg.).

([4]) Stellungnahme 8/2006 zur Überprüfung des Rechtsrahmens für elektronische Kommunikationsnetze und -dienste mit Schwerpunkt auf der Datenschutzrichtlinie für elektronische Kommunikation, angenommen am 26. September 2006.

Allgemeine Bewertung durch den EDSB

9. Insgesamt beurteilt der EDSB den Vorschlag positiv. Der EDSB befürwortet voll und ganz die Ziele, die die Kommission mit der Annahme des Vorschlags verfolgt, nämlich die Verbesserung des Schutzes der Privatsphäre und der personenbezogenen Daten der Bürger im Bereich der elektronischen Kommunikation. Der EDSB begrüßt insbesondere, dass ein obligatorisches System der Benachrichtigung bei Sicherheitsverletzungen angenommen wurde (Änderung von Artikel 4 der Datenschutzrichtlinie für die elektronische Kommunikation, mit der die Absätze 3 und 4 hinzugefügt werden). Wenn es zu Sicherheitsverletzungen kommt, hat eine Benachrichtigung deutliche Vorteile; sie stärkt die Verantwortlichkeit von Organisationen, ist ein Faktor, der Unternehmen dazu anreizt, strenge Sicherheitsmaßnahmen durchzuführen, und ermöglicht die Ermittlung der zuverlässigsten Technologien für den Schutz der Informationen. Darüber hinaus bietet sie den Betroffenen die Gelegenheit, Schritte zu unternehmen, um sich selbst vor Identitätsdiebstahl oder sonstigem Missbrauch ihrer personenbezogenen Daten zu schützen.

10. Der EDSB begrüßt andere im Vorschlag vorgesehene Änderungen wie die Möglichkeit für juristische Personen, die ein berechtigtes Interesse haben, gegen diejenigen, die gegen Bestimmungen der Datenschutzrichtlinie für die elektronische Kommunikation verstoßen, gerichtlich vorgehen zu können (Änderung des Artikels 13 durch Aufnahme des Absatzes 6). Ebenfalls positiv ist die Stärkung der Untersuchungsbefugnisse der nationalen Regulierungsbehörden, da sie dadurch in die Lage versetzt werden, zu prüfen, ob eine Datenverarbeitung rechtmäßig durchgeführt wird, und diejenigen, die Verstöße begehen, zu identifizieren (Aufnahme von Artikel 15a Absatz 3). Die Möglichkeit, unrechtmäßige Verarbeitungen personenbezogener Daten und Verletzungen der Privatsphäre so schnell wie möglich zu stoppen, ist erforderlich, damit die Rechte und Freiheiten des Einzelnen geschützt werden. Der vorgeschlagene Artikel 15a Absatz 2, in dem anerkannt wird, dass die nationalen Regulierungsbehörden befugt sind, die Einstellung von Verstößen anzuordnen, wird sehr begrüßt, da er die Regulierungsbehörden in die Lage versetzen wird, eine schwerwiegende unrechtmäßige Datenverarbeitung unverzüglich zu beenden.

11. Das Konzept des Vorschlags und die meisten der vorgeschlagenen Änderungen stehen im Einklang mit den Auffassungen über die künftige Datenschutzpolitik, die in vorherigen Stellungnahmen des EDSB geäußert wurden, so auch in der Stellungnahme über die Durchführung der Datenschutzrichtlinie ([1]). Das Konzept beruht unter anderem auf der Überzeugung, dass zwar keine neuen Datenschutzgrundsätze erforderlich sind, wohl aber spezifischere Regeln, um Datenschutzfragen anzugehen, die sich durch neue Technologien wie das Internet, RFID usw. stellen, und Instrumente, mit denen dazu beigetragen wird, Datenschutzvorschriften durchzusetzen und wirksam zu machen. Dazu gehört, dass juristische Personen in die Lage versetzt werden, gerichtlich gegen Verstöße gegen den Datenschutz vorzugehen, und die für die Verarbeitung Verantwortlichen verpflichtet werden, Sicherheitsverstöße zu melden.

12. Trotz des insgesamt positiven Konzepts des Vorschlags bedauert der EDSB, dass der Vorschlag nicht so ehrgeizig ist, wie er hätte sein können. Die Anwendung der Bestimmungen der Datenschutzrichtlinie über die elektronische Kommunikation und eine sorgfältige Analyse des Themas zeigen seit 2003, dass einige der Bestimmungen der Richtlinie bei weitem zu unklar sind, zu Rechtsunsicherheit führen und Probleme bei der Einhaltung der Richtlinie verursachen. Dies ist beispielsweise der Fall, was den Umfang betrifft, zu dem halbstaatliche Anbieter elektronischer Kommunikationsdienste von der Datenschutzrichtlinie für die elektronische Kommunikation erfasst sind. Es wäre zu hoffen gewesen, dass die Kommission die Überprüfung des Telekommunikations-Pakets, insbesondere der Datenschutzrichtlinie für die elektronische Kommunikation, nutzt, um einige der noch offenen Probleme zu lösen. Darüber hinaus bietet der Vorschlag bei neuen Aspekten wie der Einrichtung eines obligatorischen Systems der Benachrichtigung bei Sicherheitsverletzungen nur eine Teillösung, da zu den Organisationen, die verpflichtet sind, Benachrichtigungen bei Sicherheitsverletzungen vorzunehmen, nicht Stellen gehören, die sehr empfindliche Daten verarbeiten, wie beispielsweise Online-Banken oder Anbieter von Online-Gesundheitsdiensten. Der EDSB bedauert diesen Ansatz.

13. Der EDSB hofft, dass der Gesetzgeber die Bemerkungen und Vorschläge, die in dieser Stellungnahme enthalten sind, berücksichtigt, wenn der Vorschlag das Rechtsetzungsverfahren durchläuft, um die Fragen zu lösen, die in dem Kommissionsvorschlag nicht angegangen werden.

([1]) Stellungnahme des Europäischen Datenschutzbeauftragten vom 25. Juli 2007 zu der Mitteilung der Kommission an das Europäische Parlament und an den Rat mit dem Titel „Stand des Arbeitsprogramms für eine bessere Durchführung der Datenschutzrichtlinie“ (ABl. C 255 vom 27.10.2007, S. 1).

II. ANALYSE DES VORSCHLAGS

II.1. Anwendungsbereich der Datenschutzrichtlinie für die elektronische Kommunikation; insbesondere von der Richtlinie erfasste Dienste

14. Eine zentrale Frage der geltenden Datenschutzrichtlinie für die elektronische Kommunikation ist ihr Anwendungsbereich. Der Vorschlag enthält einige positive Ansatzpunkte für die Festlegung und Klärun des Anwendungsbereichs der Richtlinie, insbesondere die von der Richtlinie betroffenen Dienste, die weiter unten unter Ziffer i erörtert werden. Leider werden mit den vorgeschlagenen Änderungen nicht alle bestehenden Probleme gelöst. Wie weiter unten unter Ziffer ii erörtert, wird mit den Änderungen leider nicht bewirkt, dass der Anwendungsbereich der Richtlinie so erweitert wird, dass elektronische Kommunikationsdienste in privaten Netzen einbezogen werden.

15. In Artikel 3 der Datenschutzrichtlinie für die elektronische Kommunikation werden die von der Richtlinie erfassten Dienste beschrieben, das heißt die Dienste, für die die Verpflichtungen der Richtlinie gelten: „*Diese Richtlinie gilt für die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen*“.

16. Die von der Datenschutzrichtlinie für die elektronische Kommunikation erfassten Dienste sind daher die Anbieter öffentlicher elektronischer Kommunikationsdienste in öffentlichen Netzen. Die Definition eines Anbieters öffentlicher elektronischer Kommunikationsdienste wird in Artikel 2 Buchstabe c der Rahmenrichtlinie gegeben ([1]). Öffentliche Kommunikationsnetze werden in Artikel 2 Buchstabe d der Rahmenrichtlinie definiert ([2]). Beispiele für Tätigkeiten von Anbietern elektronischer Kommunikationsdienste sind die Bereitstellung eines Internetzugangs, die Übertragung von Informationen über elektronische Netze, Mobiltelefonverbindungen und Telefonverbindungen usw.

i) *Vorgeschlagene Änderung von Artikel 3 der Datenschutzrichtlinie für die elektronische Kommunikation: Zu den betroffenen Diensten sollen öffentlich zugängliche elektronische Kommunikationsdienste gehören, die Datenerfassungs- und Identifizierungsgeräte unterstützen*

17. Mit dem Vorschlag soll Artikel 3 der Datenschutzrichtlinie für die elektronische Kommunikation geändert werden, indem ausgeführt wird, dass zu öffentlich zugänglichen elektronischen Kommunikationsdiensten „*öffentliche Kommunikationsnetze* (gehören), *die Datenerfassungs- und Identifizierungsgeräte unterstützen*“. In Erwägungsgrund 28 wird erläutert, dass die Entwicklung von Anwendungen, die die Erfassung von Informationen einschließlich personenbezogener Daten ermöglichen und bei denen Funkfrequenzen verwendet werden, z. B. RFID-Anwendungen, der Datenschutzrichtlinie für die elektronische Kommunikation unterliegen müssen, wenn sie an öffentlich zugängliche elektronische Kommunikationsnetze oder -dienste angeschlossen sind oder solche nutzen.

18. Der EDSB hält diese Bestimmung für positiv, da sie klärt, dass eine Reihe von RFID-Anwendungen in den Anwendungsbereich der Datenschutzrichtlinie für die elektronische Kommunikation fallen, und auf diese Weise die Unsicherheit in dieser Frage beseitigt und Missverständnissen oder Missdeutungen der Rechtsvorschriften endgültig ein Ende setzt.

19. Nach dem gegenwärtig geltenden Artikel 3 der Datenschutzrichtlinie für die elektronische Kommunikation sind einige RFID-Anwendungen bereits von der Richtlinie erfasst. Dies ist aus mehreren aufeinander treffenden Gründen der Fall. Erstens fallen RFID-Anwendungen unter die Definition elektronischer Kommunikationsdienste. Zweitens aus dem Grunde, dass sie über ein elektronisches Kommunikationsnetz angeboten werden, sofern die Anwendungen von einem Übertragungssystem

([1]) Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (ABl. L 108 vom 24.4.2002, S. 33). Die Rahmenrichtlinie umreißt, was unter elektronischen Kommunikationsdiensten zu verstehen ist: i) ein „elektronischer Kommunikationsdienst“ ist ein gewöhnlich gegen Entgelt erbrachter Dienst, der in der Übertragung von Signalen über elektronische Kommunikationsnetze besteht, einschließlich Telekommunikations- und Übertragungsdienste in Netzen. ii) Dienste, die Inhalte über elektronische Kommunikationsnetze und -dienste anbieten, sind von der Definition elektronischer Kommunikationsdienste ausgenommen. iii) Bereitstellung von Diensten ist die Errichtung, der Betrieb, die Kontrolle oder die Zurverfügungstellung eines Netzes. iv) Zu elektronischen Kommunikationsdiensten gehören keine Dienste der Informationsgesellschaft, die in der Richtlinie über den elektronischen Geschäftsverkehr als Dienste definiert sind, die in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbracht werden.

([2]) Ein öffentliches Kommunikationsnetz ist ein elektronisches Kommunikationsnetz, das ganz oder überwiegend zur Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste dient.

unterstützt werden, in dem Signale drahtlos übermittelt werden. Drittens kann es sich um ein öffentliches und ein privates Netz handeln. Ist das Netz öffentlich, so werden die RFID-Anwendungen als „betroffene Dienste" gelten und daher in den Anwendungsbereich der Datenschutzrichtlinie für die elektronische Kommunikation fallen. Die vorgeschlagene Änderung wird noch verbliebene Zweifel diesbezüglich ausräumen und auf diese Weise zu mehr Rechtssicherheit führen.

20. Wie bereits in vorherigen Stellungnahmen des EDSB zu RFID ([1]) erläutert, schließt diese Bestimmung nicht aus, dass möglicherweise zusätzliche Rechtsakte in Bezug auf RFID erforderlich sind. Derartige Maßnahmen sollten jedoch in einem anderen Zusammenhang und nicht als Teil dieses Vorschlags erlassen werden.

ii) *Erfordernis, elektronische Kommunikationsdienste in privaten oder halbprivaten Netzen mit einzubeziehen*

21. Der EDSB begrüßt zwar die oben beschriebene Klärung, bedauert aber, dass in dem Vorschlag nicht auf die Problematik der sich immer weiter verwischenden Unterscheidung zwischen privaten und öffentlichen Netzen eingegangen wird. Er bedauert ferner, dass die Definition von Diensten, die von der Datenschutzrichtlinie für die elektronische Kommunikation erfasst werden, nicht so ausgeweitet wurde, dass private Netze eingeschlossen sind. Nach dem gegenwärtigen Wortlaut von Artikel 3 Absatz 1 würde die Datenschutzrichtlinie nur für *elektronische Kommunikationsdienste in öffentlichen Kommunikationsnetzen* gelten.

22. Der EDSB weist darauf hin, dass Dienste mehr und mehr eine Mischung aus privaten und öffentlichen Diensten sind. Hier sei beispielsweise auf Universitäten hingewiesen, die Tausenden Studenten die Nutzung des Internet und von E-Mail gestatten. Es liegt auf der Hand, dass sich diese halböffentlichen (oder halbprivaten) Netze auf die Privatsphäre von Personen auswirken können; diese Art von Diensten muss daher dem gleichen Regelwerk unterliegen, das auch für rein öffentliche Netze gilt. Darüber hinaus haben private Netze wie die Netze von Arbeitgebern, die Angestellten einen Internet-Zugang zur Verfügung stellen, von Hotels oder Apartmenteigentümern, die Gästen Telefon und E-Mail zur Verfügung stellen, sowie von Internet-Cafés Auswirkungen auf den Schutz von Daten und der Privatsphäre ihrer Nutzer; sie sollten daher ebenfalls vom Anwendungsbereich der Datenschutzrichtlinie für die elektronische Kommunikation erfasst werden.

23. Nach der Rechtsprechung einiger Mitgliedstaaten unterliegen elektronische Kommunikationsdienste in privaten Netzen bereits den gleichen Verpflichtungen wie Dienste in öffentlichen Netzen ([2]). Auch nach deutschem Recht sind Datenschutzbehörden zu der Auffassung gelangt, dass das Gestatten der privaten E-Mail-Nutzung in einem Unternehmen dazu führen kann, dass das Unternehmen als Betreiber eines öffentlichen Telekommunikationsdienstes gelten muss und daher die Bestimmungen der Datenschutzrichtlinie für die elektronische Kommunikation für das Unternehmen gelten müssen.

24. Kurz gesagt rechtfertigt die wachsende Bedeutung gemischter (privater/öffentlicher) und privater Netze im täglichen Leben mit entsprechend steigendem Risiko für personenbezogene Daten und die Privatsphäre, dass für solche Dienste das gleiche Regelwerk gelten muss wie für öffentliche elektronische Kommunikationsdienste. Der EDSB ist daher der Auffassung, dass der Anwendungsbereich der Richtlinie so geändert werden sollte, dass solche privaten Dienste eingeschlossen sind; diese Auffassung wird von der Datenschutzgruppe „Artikel 29" geteilt ([3]).

II.2. **Benachrichtigung über Sicherheitsverletzungen: Änderung von Artikel 4**

25. Artikel 4 der Datenschutzrichtlinie für die elektronische Kommunikation soll durch Anfügung von zwei neuen Absätzen (Absätze 3 und 4), die eine Verpflichtung zur Meldung von Sicherheitsverletzungen enthalten, geändert werden. Nach Artikel 4 Absatz 3 sind Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste zum einen verpflichtet, der nationalen Regulierungsbehörde unverzüglich eine Sicherheitsverletzung, die zur zufälligen oder unrechtmäßigen Zerstörung, zu Verlust, Veränderung, unbefugter Weitergabe oder unberechtigtem Zugang zu übermittelten, gespeicherten oder anderweitig verarbeiteten personenbezogenen Daten im Zusammenhang mit der Bereitstellung öffentlich zugänglicher Kommunikationsdienste („Datengefährdung") führt, zu melden; zum anderen sind sie auch verpflichtet, ihre Kunden zu benachrichtigen.

([1]) Stellungnahme des Europäischen Datenschutzbeauftragten vom 20. Dezember 2007 zu der Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen zum Thema „Funkfrequenzkennzeichnung (RFID) in Europa: Schritte zu einem ordnungspolitischen Rahmen" (KOM(2007) 96).

([2]) Beispielsweise hat der Appellationshof Paris in seinem Urteil in der Rechtssache *BNP Paribas* gegen *World Press Online* vom 4. Februar 2005 befunden, dass es keinen Unterschied zwischen Internet-Diensteanbietern, die auf kommerzieller Basis Internet-Zugang anbieten, und Arbeitgebern gibt, die ihrem Personal einen Internet-Zugang zur Verfügung stellen.

([3]) Stellungnahme 8/2006 zur Überprüfung des Rechtsrahmens für elektronische Kommunikationsnetze und -dienste mit Schwerpunkt auf der Datenschutzrichtlinie für elektronische Kommunikation, angenommen am 26. September 2006.

Vorteile dieser Verpflichtung

26. Der EDSB begrüßt diese Bestimmungen (Artikel 4 Absätze 3 und 4), mit denen eine Meldepflicht für Sicherheitsverletzungen eingeführt wird. Die Meldung von Sicherheitsverletzungen wirkt sich positiv auf den Schutz personenbezogener Daten und der Privatsphäre aus; dies ist bereits in den Vereinigten Staaten erprobt worden, wo schon seit einigen Jahren Rechtsvorschriften auf nationaler Ebene für die Meldung von Sicherheitsverletzungen gelten.

27. Erstens verbessern Rechtsvorschriften für die Meldung von Sicherheitsverletzungen die Verantwortlichkeit von Betreibern öffentlich zugänglicher elektronischer Kommunikationsdienste für die Daten, bei denen eine Sicherheitsverletzung vorliegt. Nach dem Ordnungsrahmen für den Schutz von Daten und der Privatsphäre bedeutet Verantwortlichkeit, dass jede Organisation für die Daten verantwortlich ist, die sich in ihrer Obhut und unter ihrer Aufsicht befinden. Die Meldepflicht ist gleichbedeutend mit einer Bestätigung, dass sich zum einen die Daten, bei denen eine Sicherheitsverletzung vorliegt, unter der Aufsicht des Betreibers öffentlich zugänglicher elektronischer Kommunikationsdienste befunden haben, und zum anderen, dass diese Organisation dafür verantwortlich ist, für solche Daten die erforderlichen Maßnahmen zu ergreifen.

28. Zweitens hat sich herausgestellt, dass eine Meldepflicht für Sicherheitsverletzungen ein Faktor ist, der Organisationen, die personenbezogene Daten verarbeiten, zu Investitionen in die Sicherheit veranlasst. Allein der Umstand, dass Sicherheitsverletzungen öffentlich mitgeteilt werden müssen, veranlasst Organisationen dazu, strengere Sicherheitsstandards für den Schutz personenbezogener Daten und zur Verhinderung von Sicherheitsverletzungen anzuwenden. Darüber hinaus wird die Meldung von Sicherheitsverletzungen dazu beitragen, dass verlässliche statistische Analysen hinsichtlich der wirksamsten Sicherheitslösungen und -mechanismen definiert und durchgeführt werden. Es gab sehr lange zu wenige belastbare Daten über Mängel bei der Informationssicherheit und über die besten Technologien zum Schutz der Informationen. Das Problem wird voraussichtlich mit der Meldpflicht für Sicherheitsverletzungen gelöst, so wie dies auch der Fall infolge der US-Gesetze für die Meldepflicht für Sicherheitsverletzungen war, da die Meldungen Erkenntnisse über die Technologien liefern, die Sicherheitsverletzungen eher begünstigen ([1]).

29. Außerdem wird der Einzelne durch die Benachrichtigung über Sicherheitsverletzungen über die Risiken aufgeklärt, die bestehen, wenn es bei seinen personenbezogenen Daten zu einer Sicherheitsverletzung kommt; dies trägt dazu bei, dass sie die erforderlichen Maßnahmen zur Minderung solcher Risiken ergreifen. Beispielsweise kann sich ein Bürger, bei dessen Bankdaten eine Sicherheitsverletzung vorliegt und der darüber unterrichtet wird, entscheiden, die Zugangsdaten für sein Konto zu ändern, um zu verhindern, dass sich Dritte diese Angaben beschaffen und für illegale Zwecke nutzen (üblicherweise als „Identitätsdiebstahl" bezeichnet). Alles in allem verringert die Meldepflicht die Wahrscheinlichkeit, dass der Einzelne Opfer von Identitätsdiebstahl wird, und hilft darüber hinaus den Opfern möglicherweise dabei, die für die Lösung des Problems erforderlichen Maßnahmen zu treffen.

Mängel der vorgeschlagenen Änderung

30. Der EDSB ist zwar über das in Artikel 4 Absätze 3 und 4 festgelegte System der Meldung von Sicherheitsverletzungen erfreut, hätte aber begrüßt, wenn das System auf breiterer Basis angewandt würde und Anbieter von Diensten der Informationsgesellschaft mit einbezogen wären. Dies würde bedeuten, dass Online-Banken, Online-Unternehmen, Online-Anbieter von Gesundheitsdiensten usw. ebenfalls von den Rechtsvorschriften erfasst wären ([2]).

31. Eine Meldepflicht für Sicherheitsverletzungen für Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste ist auch hinsichtlich anderer Organisationen gerechtfertigt, die große Mengen personenbezogener Daten verarbeiten, deren Offenlegung für die Betroffenen besonders schädlich sein könnte. Dazu gehören Online-Banken, Datenvermittler und andere Online-Anbieter, die sensible Daten verarbeiten (unter anderem Gesundheitsdaten, Daten über politische Auffassungen usw.). Die Offenlegung von Informationen, die von Online-Banken und Online-Unternehmen verwaltet werden und zu denen nicht nur Bankkontonummern, sondern auch Kreditkartendaten gehören können, kann zu einem Identitätsdiebstahl führen; in diesem Fall ist es für die Betroffenen wichtig, dass sie benachrichtigt werden, damit sie die erforderlichen Maßnahmen treffen können. Im letztgenannten Fall (Online-Gesundheitsdienste) geht es vielleicht nicht um eine finanzielle Schädigung, aber die Betroffenen werden aller Voraussicht nach einen moralischen Schaden erleiden, wenn sensible Informationen offen gelegt werden.

([1]) Siehe den Bericht „*Security Economics and the Internal Market*" von Prof. Ross Anderson, Rainer Böhme, Richard Clayton und Tyler Moore, der von der ENISA in Auftrag gegeben wurde. Der Bericht ist auf folgender Website abrufbar: http://www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf

([2]) Dienste der Informationsgesellschaft sind in der Richtlinie über den elektronischen Geschäftsverkehr als Dienstleistungen definiert, die in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbracht werden.

32. Durch eine Ausweitung des Anwendungsbereichs der Meldepflicht wären darüber hinaus die oben beschriebenen Vorteile, die durch eine Meldepflicht zu erwarten sind, nicht auf einen Branchenbereich, nämlich den der Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste, beschränkt, sondern kämen allgemein den Diensten der Informationsgesellschaft zugute. Die Meldepflicht für Sicherheitsverletzungen für Dienste der Informationsgesellschaft wie z. B. Online-Banken wird nicht nur ihre Verantwortlichkeit erhöhen, sondern wird sie auch dazu veranlassen, ihre Sicherheitsmaßnahmen zu verbessern und auf diese Weise etwaige künftige Sicherheitsverletzungen zu verhindern.

33. Es gibt ähnlich gelagerte Fälle, in denen die Datenschutzrichtlinie für die elektronische Kommunikation bereits für andere Stellen als die Anbieter öffentlicher elektronischer Kommunikationsdienste gilt, etwa Artikel 5 zur Vertraulichkeit der Kommunikation und Artikel 13 zu unerbetener Werbung („Spam"). Dies bestätigt, dass der Gesetzgeber in der Vergangenheit vorausschauend beschlossen hat, den Anwendungsbereich bestimmter Vorschriften der Datenschutzrichtlinie für die elektronische Kommunikation auszuweiten, da dies seines Erachtens sinnvoll und notwendig war. Der Europäische Datenschutzbeauftragte hofft, dass der Gesetzgeber auch jetzt nicht zögern wird, genauso sinnvoll und flexibel vorzugehen und den Anwendungsbereich des Artikels 4 auszudehnen, um die Anbieter von Diensten der Informationsgesellschaft mit einzubeziehen. Zu diesem Zweck würde es ausreichen, in Artikel 4 Absatz 3 folgendermaßen auf solche Anbieter Bezug zu nehmen: „*Im Fall einer Sicherheitsverletzung* (…), (muss) *der Betreiber der öffentlich zugänglichen elektronischen Kommunikationsdienste* und der Betreiber der Dienste der Informationsgesellschaft *den betroffenen Teilnehmer und die nationale Regulierungsbehörde unverzüglich von der Sicherheitsverletzung benachrichtigen*".

34. Der EDSB betrachtet diese Verpflichtung und ihre Anwendung sowohl auf die Anbieter öffentlicher elektronischer Kommunikationsdienste als auch auf die Betreiber von Diensten der Informationsgesellschaft als ersten Schritt einer Entwicklung, die in Zukunft all jene, die für die Verarbeitung von Daten verantwortlich sind, mit einschließen könnte.

Gesonderter Rechtsrahmen für die Regelung von Sicherheitsverletzungen im Wege von Ausschussverfahren

35. Eine Reihe von Fragen im Zusammenhang mit der Meldepflicht bei Sicherheitsverletzungen bleiben in dem Vorschlag unberücksichtigt. Anzusprechende Punkte wären etwa Umstände, Form und Verfahren der entsprechenden Benachrichtigung. Stattdessen bleibt dem Vorschlag zufolge der Erlass solcher Maßnahmen einem „Komitologie"-Ausschuss ([1]) überlassen, nämlich dem durch Artikel 22 der Rahmenrichtlinie eingesetzten Kommunikationsausschuss nach dem Verfahren des Ratsbeschlusses vom 28. Juni 1999. Der Erlass solcher Maßnahmen soll insbesondere im Verfahren nach Artikel 5 des Ratsbeschlusses vom 28. Juni 1999 erfolgen, der Vorschriften für das Regelungsverfahren bei „*Maßnahmen von allgemeiner Tragweite, mit denen wesentliche Bestimmungen von Basisrechtsakten angewandt werden sollen*" enthält.

36. Der EDSB spricht sich nicht gegen die Entscheidung aus, all diese Punkte im Rahmen der Durchführungsvorschriften zu regeln. Die Annahme von Rechtsvorschriften im Ausschussverfahren führt wahrscheinlich zu einer Verkürzung des Legislativverfahrens. Auch trägt das Ausschussverfahren zur Harmonisierung bei, die es in jedem Fall anzustreben gilt.

37. Angesichts der großen Zahl der in den Durchführungsmaßnahmen zu regelnden Fragen und ihrer Bedeutung, die bereits angesprochen wurde, scheint es sinnvoll zu sein, alle Punkte gemeinsam in einem einzigen Rechtsetzungsakt zu behandeln und nicht fragmentarisch vorzugehen und etwa einige Punkte in der Datenschutzrichtlinie für die elektronische Kommunikation, andere wiederum erst im Rahmen der Durchführungsvorschriften zu regeln. Der Ansatz der Kommission, wonach diese Entscheidungen Gegenstand der Durchführungsbestimmungen sein sollen, die nach Anhörung des Datenschutzbeauftragten — und hoffentlich weiterer interessierter Kreise (siehe unten) — festzulegen sind, ist daher zu begrüßen.

Im Rahmen von Durchführungsmaßnahmen zu regelnde Fragen

38. Die Bedeutung der Durchführungsmaßnahmen ist klar erkennbar, wenn man vorab die Punkte, die im Rahmen solcher Maßnahmen zu regeln sind, im Einzelnen betrachtet. So können in den Durchführungsmaßnahmen die Standards vorgegeben werden, die für die Meldungen gelten sollen. Beispielsweise wird darin angegeben, wann eine Sicherheitsverletzung vorliegt, unter welchen Bedingungen die Benachrichtigung von Einzelpersonen und Behörden zu erfolgen hat und welche Fristen für Meldung und Benachrichtigung gelten.

([1]) EG-Rechtsetzungsverfahren im Rahmen von Ausschüssen, die sich aus Regierungsvertretern der Mitgliedstaaten auf Beamtenebene zusammensetzen.

39. Der EDSB vertritt die Auffassung, dass die Datenschutzrichtlinie für die elektronische Kommunikation und insbesondere ihr Artikel 4 keinerlei Ausnahmen von der Meldepflicht vorsehen sollten. Er begrüßt daher den von der Kommission gewählten Ansatz, wonach Artikel 4 die Meldepflicht — ohne Ausnahme — festschreibt, wobei diese und andere Fragen dann im Rahmen der Durchführungsbestimmungen zu regeln sind. Zwar sind dem EDSB die Argumente bekannt, die gewisse Ausnahmen von der Meldepflicht rechtfertigen könnten, doch sollten diese und andere Fragen im Rahmen der Durchführungsbestimmungen im Einzelnen geklärt werden, nachdem alle anstehenden Fragen eingehend und umfassend erörtert worden sind. Wie bereits erwähnt, lässt es die Komplexität der Fragen im Zusammenhang mit der Meldepflicht bei Sicherheitsverletzungen, einschließlich der Frage, ob Ausnahmen oder Einschränkungen sachdienlich sind, angezeigt erscheinen, dies in vereinheitlichter Form zu regeln, das heißt in einem gesonderten Rechtsetzungsakt, in dem ausschließlich dieser Punkt behandelt wird.

Anhörung des Europäischen Datenschutzbeauftragten; notwendigkeit von Konsultationen auf breiterer Ebene

40. Angesichts des Ausmaßes, in dem sich die Durchführungsmaßnahmen auf den Schutz der personenbezogenen Daten von Einzelnen auswirken, ist es von großer Wichtigkeit, dass die Kommission vor dem Erlass dieser Maßnahmen in angemessener Form Konsultationen durchführt. Der EDSB begrüßt daher Artikel 4 Absatz 4 des Vorschlags, in dem explizit festgelegt wird, dass der EDSB vor Erlass von Durchführungsmaßnahmen von der Kommission konsultiert wird. Diese Maßnahmen haben nicht nur den Schutz personenbezogener Daten und die Privatsphäre des Einzelnen zum Gegenstand, sondern sie beeinflussen diesen Bereich auch in hohem Maße. Daher ist es wichtig, dass — wie in Artikel 41 der Verordnung (EG) Nr. 45/2001 vorgeschrieben — die Stellungsnahme des EDSB eingeholt wird.

41. Zusätzlich zu der Konsultation des EDSB kann es zweckdienlich sein, eine Bestimmung einzufügen, wonach über den Entwurf von Durchführungsmaßnahmen eine Anhörung der Öffentlichkeit stattfindet, um fachlichen Rat einzuholen und den Austausch von Informationen über bewährte Praktiken in diesem Bereich zu fördern. Hierdurch würde ein geeigneter Kommunikationsweg geschaffen, auf dem nicht nur die Branche, sondern auch andere interessierte Kreise wie etwa andere Datenschutzstellen und die Datenschutzgruppe „Artikel 29" ihre Meinungen zu Gehör bringen könnten. In noch stärkerem Maße scheint eine Anhörung der Öffentlichkeit notwendig zu sein, wenn man bedenkt, dass die Rechtsetzung im Rahmen des Ausschussverfahrens erfolgt und das Europäische Parlament nur begrenzte Mitsprachemöglichkeiten hat.

42. Der EDSB stellt fest, dass in Artikel 4 Absatz 4 vorgesehen ist, dass die Kommission vor dem Erlass von Durchführungsvorschriften auch die Europäische Behörde für die Märkte der elektronischen Kommunikation konsultiert. Der EDSB würdigt in diesem Zusammenhang das Prinzip der Konsultation dieser Behörde als Träger der Erfahrungen und des Fachwissens der ENISA in Fragen der Netz- und Informationssicherheit. Bis zur Errichtung der Europäischen Behörde für die Märkte der elektronischen Kommunikation könnte es als Zwischenlösung sinnvoll sein, in der vorgeschlagenen Änderung (Artikel 4 Absatz 4) eine Konsultation der ENISA vorzusehen.

II.3. **Bestimmung über Cookies, Spyware und ähnliche Instrumente: Änderung von Artikel 5 Absatz 3**

43. Artikel 5 Absatz 3 der Datenschutzrichtlinie behandelt die Frage von Technologien, die den Zugriff auf Informationen und die Speicherung von Informationen, die im Endgerät des Nutzers gespeichert sind, über elektronische Kommunikationsdienste erlauben. Ein Beispiel für die Anwendung von Artikel 5 Absatz 3 ist der Einsatz von Cookies ([1]). Zu weiteren Beispielen zählt unter anderem die Nutzung von Technologien wie Spyware (verborgene Spionageprogramme) und Trojanern (Programme, die sich in elektronischen Botschaften oder in anderer dem Anschein nach harmloser Software verstecken). Diese Technologien und Anwendungen verfolgen höchst unterschiedliche Ziele, bei denen einige als völlig harmlos oder sogar hilfreich für den Nutzer anzusehen sind, während andere sich ganz eindeutig als sehr schädlich und bedrohlich erweisen.

([1]) „Cookies" werden von ISSP (Websites) in den Endgeräten der Nutzer zu verschiedenen Zwecken gesetzt, unter anderem zur Erkennung eines Nutzers, wenn er erneut eine Website besucht. In der Praxis sieht das so aus, dass in dem Augenblick, in dem eine von einem Internetnutzer besuchte Website ein Cookie an den Rechner dieses Nutzers sendet, diesem Rechner eine unverwechselbare Nummer zugeteilt wird (d. h. der Rechner, der ein bestimmtes Cookie von der Website A empfangen hat, ist jetzt als „Rechner, auf dem das Cookie 111 abgelegt ist" identifiziert). Die Website bewahrt diese Nummer als Referenz auf. Falls der Nutzer des Rechners, auf dem Cookie 111 abgelegt wurde, die Cookie-Datei nicht löscht, kann die betreffende Website den Rechner bei seinem nächsten Besuch auf derselben Website stets als Inhaber von Cookie 111 identifizieren. Die Website folgert daraus natürlich, dass dieser Rechner sie schon bei früheren Gelegenheiten besucht hat. Der Mechanismus, der einer Website die Erkennung eines Nutzers als Wiederholungsbesucher erlaubt, ist ganz einfach. Wenn auf einem bestimmten Rechner Cookies wie etwa Cookie 111 abgelegt sind und dieser Rechner die Website besucht, die bei einem früheren Besuch dieses bestimmte Cookie generiert hat, sucht er die Festplatte des Nutzers nach der zugehörigen Cookie-Dateinummer ab. Wenn der Browser des Nutzers eine Cookie-Datei findet, die zu der auf der Website gespeicherten Referenznummer passt, informiert er die Website, dass auf dem Rechner Cookie 111 abgelegt ist.

44. Artikel 5 Absatz 3 der Datenschutzrichtlinie legt die Bedingungen fest, die gelten, wenn es um den Zugriff auf Informationen oder die Speicherung von Informationen im Endgerät des Nutzers unter anderem mittels der zuvor beschriebenen Technologien geht. Nach Artikel 5 Absatz 3 gilt insbesondere Folgendes: i) Internetnutzer müssen gemäß der Richtlinie 95/46/EG klare und umfassende Informationen insbesondere über die Zwecke der Verarbeitung erhalten, und ii) Internetnutzern muss zugestanden werden, diese Verarbeitung zu verweigern, d. h. die Verarbeitung der aus ihren Endgeräten ausgelesenen Informationen ganz einfach abzulehnen.

Vorteile der vorgeschlagenen Änderung

45. Der geltende Artikel 5 Absatz 3 der Datenschutzrichtlinie beschränkt deren Anwendungsbereich auf Fälle, in denen der Zugriff auf Informationen und die Speicherung von Informationen im Endgerät des Nutzers über *elektronische Kommunikationsnetze* erfolgen. Dies schließt den zuvor beschriebenen Fall des Einsatzes von Cookies sowie anderer Technologien wie Spyware ein, die über elektronische Kommunikationsnetze übertragen werden. Es ist jedoch überhaupt nicht klar, ob Artikel 5 Absatz 3 in Fällen Anwendung findet, in denen vergleichbare Technologien (Cookies, Spyware und Ähnliches) über Software auf externen Speichermedien bereitgestellt und in das Endgerät des Nutzers heruntergeladen werden. Da die Bedrohung der Privatsphäre unabhängig vom Übermittlungskanal gegeben ist, erweist sich die Beschränkung von Artikel 5 Absatz 3 auf nur einen Übermittlungskanal als recht unglücklich.

46. Der EDSB begrüßt daher die Änderung von Artikel 5 Absatz 3, mit der durch die Streichung der Bezugnahme auf „elektronischer Kommunikationsnetze" in der Tat der Geltungsbereich von Artikel 5 Absatz 3 erweitert wird. Der geänderte Wortlaut von Artikel 5 Absatz 3 umfasst damit die beiden Fälle, in denen nämlich der Zugriff auf Informationen und die Speicherung von Informationen im Endgerät des Nutzers über elektronische Kommunikationsnetze, aber auch über andere externe Speichermedien wie CD, CD-ROM, USB-Stick usw. erfolgen.

Technische Speicherung zur Erleichterung der Übertragung

47. Der letzte Satz von Artikel 5 Absatz 3 der Datenschutzrichtlinie für die elektronische Kommunikation in seiner geänderten Fassung bleibt unverändert. Diesem Satz zufolge stehen die Bestimmungen von Artikel 5 Absatz 3 Satz 1 „*einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung oder Erleichterung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist oder, soweit dies unbedingt erforderlich ist, um einen (…) Dienst der Informationsgesellschaft zur Verfügung zu stellen*". Somit gelten die verbindlichen Vorschriften von Artikel 5 Absatz 3 Satz 1 (Informationspflicht und Hinweis auf das Verweigerungsrecht) dann nicht, wenn der alleinige Zweck des Zugangs zu Endgeräten des Nutzers oder der Speicherung von Informationen darin besteht, eine Übertragung zu *erleichtern* oder soweit dies unbedingt erforderlich ist, um einen vom Nutzer ausdrücklich gewünschten Dienst der Informationsgesellschaft zur Verfügung zu stellen.

48. In der Richtlinie wird nicht erläutert, wann Zugang oder Speicherung allein zum Zweck der Erleichterung einer Übertragung oder der Bereitstellung von Informationen erfolgen. Ein Fall, der eindeutig unter diese Ausnahmeregelung fallen würde, ist die Einrichtung eines Internetanschlusses. Grund dafür ist, dass die Einrichtung eines Internetanschlusses erforderlich ist, um eine IP-Adresse zu erhalten ([1]). Beim Computer des Nutzers werden bestimmte diesen Computer betreffende Informationen abgefragt, die er dem Anbieter des Internetzugangs gegenüber offen legt, und im Gegenzug wird ihm durch den Anbieter eine IP-Adresse zugeteilt. Somit wird die im Endgerät des Nutzers gespeicherte Information zum Anbieter zu dem Zweck übertragen, dem Nutzer einen Internetzugang zur Verfügung zu stellen. In diesem Fall hat der Anbieter nicht die Pflicht, auf diese Erfassung von Informationen hinzuweisen und ein Verweigerungsrecht einzuräumen, da er Datenzugriff für die Bereitstellung des Dienstes erforderlich ist.

49. Wenn der Internetanschluss eingerichtet ist, muss ein Nutzer, der eine bestimmte Website besuchen will, eine Anfrage an den Server richten, der diese Website anbietet. Die Antwort des Servers erfolgt, sofern dieser weiß, wohin er die Information zu senden hat, das heißt, sofern er die IP-Adresse des Nutzers kennt. Aufgrund der Art der Speicherung dieser Adresse ist es erneut erforderlich, dass die Website, die der Nutzer besuchen will, auf Informationen auf dem Endgerät des Internetnutzers zugreift. Dieser Vorgang würde ebenfalls klar unter die Ausnahmeregelung fallen. Es scheint durchaus zweckmäßig, dass die genannten Fälle nicht in den Anwendungsbereich der Anforderungen nach Artikel 5 Absatz 3 fallen.

([1]) Bei einer IP (Internet Protocol)-Adresse handelt es sich um eine nur einmal vergebene Adresse, die von bestimmten elektronischen Geräten zur gegenseitigen Identifizierung und Kommunikation in ein Computernetz genutzt wird, das auf dem Internet Protocol (IP)-Standard basiert — einfacher gesagt, um die Adresse des Computers. Jedes Gerät im Netz — hierzu zählen Router, Switches, Computer, Infrastrukturserver (z. B. NTP, DNS, DHCP, SNMP usw.), Drucker, Internetfaxgeräte und einige Telefone — kann eine eigene, im Bereich des jeweiligen Netzes unverwechselbare Adresse haben. Einige IP-Adressen sind so angelegt, dass sie im Gesamtbereich des Internet einzigartig sind, andere müssen lediglich innerhalb eines Netzwerks einzigartig sein.

50. Der EDSB hält es für zweckmäßig, Ausnahmen von der Informationspflicht und dem Verweigerungsrecht in Fällen wie den genannten vorzusehen, wenn die technische Speicherung oder der Zugang zum Endgerät eines Nutzers ausschließlich zum Zweck der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz *erforderlich* ist. Das Gleiche gilt für die Fälle, in denen die technische Speicherung oder der Zugang unbedingt erforderlich ist, um einen Dienst der Kommunikationsgesellschaft zur Verfügung zu stellen. Eine solche Ausnahmeregelung ist nach Auffassung des EDSB nicht erforderlich, wenn die technische Speicherung oder der Zugang lediglich die *Erleichterung* der Übertragung einer Nachricht zum Zweck hat. So könnte es beispielsweise aufgrund des letzten Satzes dieses Artikels dazu kommen, dass eine betroffene Person nicht informiert wird und nicht das Recht geltend machen kann, die Verarbeitung ihrer Daten zu verweigern, wenn ihre Sprachpräferenzen oder ihr Standort (z. B. Belgien oder China) in einem Cookie erfasst werden, da angeführt werden könnte, dass mit einem solchen Cookie die Übertragung einer Nachricht erleichtert werden soll. Der EDSB ist sich dessen bewusst, dass die betroffenen Personen in der Praxis die Möglichkeit haben, die Speicherung von Cookies auf Ebene der Software zu verweigern oder individuell einzustellen. Diese Möglichkeit ist jedoch nicht klar genug in einer Rechtsvorschrift verankert, die die betroffene Person förmlich berechtigt, ihre Rechte in dem beschriebenen Zusammenhang geltend zu machen.

51. Um diese Auswirkung zu vermeiden, schlägt der EDSB eine geringfügige Änderung am Ende des Artikels 5 Absatz 3 vor, nämlich die Streichung des Wortes „Erleichterung": „*(…) steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung oder* Erleichterung *der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist oder, soweit dies unbedingt erforderlich ist, um einen (…) Dienst der Informationsgesellschaft zur Verfügung zu stellen*".

II.4. **Klagen von Anbietern elektronischer Kommunikationsdienste in öffentlich zugänglichen Netzen und juristischen Personen: Hinzufügung von Absatz 6 zu Artikel 13**

52. Der vorgeschlagene Artikel 13 Absatz 6 sieht zivilrechtliche Mittel für natürliche und juristische Personen vor, die ein berechtigtes Interesse an der Bekämpfung von Verstößen gegen Artikel 13 der Datenschutzrichtlinie für die elektronische Kommunikation haben, insbesondere Anbieter elektronischer Kommunikationsdienste, die ihre Geschäftsinteressen schützen wollen. Bei diesem Artikel geht es um die Versendung unerbetener Werbung.

53. Nach der vorgeschlagenen Änderung können beispielsweise Anbieter von Internet-Zugängen gegen Spam-Versender wegen Missbrauchs ihrer Netze oder gegen Stellen, die Sender-Adressen fälschen oder Server hacken, um sie als Spam-Relays zu missbrauchen, gerichtlich vorgehen.

54. Aus der Datenschutzrichtlinie für die elektronische Kommunikation ging vorher nicht eindeutig hervor, ob Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste das Recht haben, gegen Spam-Versender vorzugehen, und es gibt nur sehr wenige Fälle, in denen Anbieter bei Gericht wegen eines Verstoßes gegen die einzelstaatliche Rechtsvorschrift, mit der Artikel 13 umgesetzt wird, Klage erhoben haben ([1]). Dadurch, dass in dem Vorschlag das Recht der Anbieter elektronischer Kommunikationsdienste anerkannt wird, ihre Geschäftsinteressen auf dem Rechtsweg zu schützen, wird bestätigt, dass die Datenschutzrichtlinie für die elektronische Kommunikation nicht nur einzelne Teilnehmer sondern auch die Anbieter elektronischer Kommunikationsdienste schützen soll.

55. Der EDSB begrüßt, dass der Vorschlag für Anbieter elektronischer Kommunikationsdienste, die ein geschäftliches Interesse daran haben, die Möglichkeit einführt, gerichtlich gegen Spam-Versender vorzugehen. Einzelne Teilnehmer haben in der Regel weder das Geld, um eine solches Verfahren anzustrengen, noch würde es ihnen Vorteile bringen. Die Anbieter von Internet-Zugängen und andere Anbieter elektronischer Kommunikationsdienste hingegen haben die Finanzkraft und sind technisch dazu in der Lage, Spam-Kampagnen zu untersuchen und die Täter zu identifizieren; und es scheint nur billig zu sein, dass sie das Recht haben, gerichtlich gegen Spam-Versender vorzugehen.

56. Der EDSB hält die vorgeschlagene Änderung vor allem insofern für wichtig, als sie es Verbraucherverbänden und Gewerkschaften, die die Interessen Spam-geschädigter Verbraucher vertreten, ermöglichen würde, in deren Namen vor Gericht zu gehen. Wie oben dargelegt, ist der Schaden, den eine Spam-Geschädigter erleidet, im Einzelfall als solcher nicht groß genug, um deswegen rechtliche Schritte einzuleiten. Der EDSB hat die gleiche Maßnahme im Prinzip bereits in seiner Stellungnahme zum Stand

([1]) Ein solcher Fall ist die Rechtssache *Microsoft Corporation* gegen *Paul McDonald t/a Bizards UK* (2006 All Er (D) 153).

des Arbeitsprogramms zur besseren Durchführung der Datenschutzrichtlinie ([1]) für Verstöße gegen den Datenschutz vorgeschlagen, die eine Verletzung der Privatsphäre darstellen. Nach Ansicht des EDSB hätte der Vorschlag noch weiter gehen können und Verbandsklagen vorschlagen können, mit denen Gruppen von Bürgern gemeinsam in Datenschutzangelegenheiten den Rechtsweg beschreiten können. Im Falle von Spam, wo ja eine große Zahl von Einzelpersonen betroffen sind, besteht ein Potenzial dafür, dass sich Gruppen von Einzelpersonen zusammentun, um eine Verbandsklage gegen Spam-Versender anzustrengen.

57. Der EDSB bedauert besonders, dass der Vorschlag die Möglichkeit rechtlicher Maßnahmen für juristische Personen auf Situationen beschränkt, in denen gegen Artikel 13 der Richtlinie verstoßen wird, d. h. Situationen, in denen die Bestimmung über unerbetene E-Mails verletzt werden. Die vorgeschlagene Änderung erlaubt keine rechtlichen Schritte juristischer Personen bei Verstößen gegen andere Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation. So gibt die Bestimmung in der derzeitigen Fassung einer juristischen Person — beispielsweise einer Verbraucherorganisation — nicht das Recht, gerichtlich gegen einen Internet-Anbieter vorzugehen, der persönliche Daten von Millionen von Verbrauchern weitergegeben hat. Die Durchsetzung der Datenschutzrichtlinie für elektronische Kommunikation insgesamt — nicht nur eines bestimmten Artikels — wäre wesentlich besser, wenn die Bestimmung des Artikels 13 Absatz 6 zu einer allgemeinen Bestimmung gemacht würde, die juristischen Personen das Recht gibt, gegen Verstöße gegen gleich welche Bestimmung der Datenschutzrichtlinie für elektronische Kommunikation rechtlich vorzugehen.

58. Um dieses Problem zu lösen, schlägt der EDSB vor, aus Artikel 13 Absatz 6 einen gesonderten Artikel zu machen (Artikel 14) und den Wortlaut von Artikel 13 Absatz 6 geringfügig dahin gehend zu ändern, dass die Worte „aufgrund dieses Artikels“ durch die Worte „aufgrund dieser Richtlinie“ ersetzt werden.

II.5. **Verschärfung der Bestimmungen zur Durchsetzung: Hinzufügung von Artikel 15a**

59. Die Datenschutzrichtlinie für elektronische Kommunikation enthält keine ausdrücklichen Bestimmungen zur Durchsetzung. Sie verweist statt dessen auf den Abschnitt zur Durchsetzung in der Datenschutzrichtlinie ([2]). Der EDSB begrüßt den vorgeschlagenen neuen Artikel 15a, in dem Fragen der Durchsetzung ausdrücklich geregelt werden.

60. Zunächst einmal stellt der EDSB fest, dass — eine wirksame Durchsetzungsstrategie in diesem Bereich voraussetzt (wie in dem vorgeschlagenen Artikel 15a Absatz 3 verlangt wird) — die nationalen Behörden die nötigen Untersuchungsbefugnisse haben, um die erforderlichen Informationen sammeln zu können. Sehr oft liegen die Beweise für Verstöße gegen die Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation in elektronischer Form vor und können auf verschiedenen Computern und Geräten oder Netzen gespeichert sein. In diesem Zusammenhang ist es wichtig, dass den für die Durchsetzung zuständigen Stellen die Möglichkeit eingeräumt wird, Durchsuchungsbefehle zu erhalten, die ihnen die Befugnis zum Zugang, zur Durchsuchung und zur Beschlagnahme geben.

61. Zweitens begrüßt der EDSB ganz besonders die in Artikel 15a Absatz 2 vorgeschlagene Änderung, wonach der die nationalen Regulierungsbehörden Verfügungsbefugnis haben müssen, d. h. befugt sein müssen, die Einstellung von Verstößen anzuordnen, und wonach sie über die erforderlichen Untersuchungsbefugnisse und Mittel verfügen müssen. Die nationalen Regulierungsbehörden, darunter die nationalen Datenschutzbehörden, müssen befugt sein, Verfügungen auszusprechen, die diejenigen, die gegen die Vorschriften verstoßen, verpflichten, eine gegen die Datenschutzrichtlinie für elektronische Kommunikation verstoßende Tätigkeit einzustellen. Verfügungen oder die Befugnis, die Einstellung eines Verstoßes anzuordnen, sind ein nützliches Instrument bei anhaltenden Verstößen gegen individuelle Rechte. Verfügungen werden sehr nützlich sein, wenn es darum geht, Verstößen gegen die Datenschutzrichtlinie für elektronische Kommunikation wie beispielsweise Verstöße gegen Artikel 13 betreffend unerbetene Werbung, die naturgemäß anhaltende Verstöße sind, zu unterbinden.

62. Drittens versetzt der Vorschlag die Kommission in die Lage, technische Durchführungsmaßnahmen zu treffen, um eine wirksame grenzüberschreitende Zusammenarbeit bei der Durchsetzung einzelstaatlicher Rechtsvorschriften sicherzustellen (in Artikel 15a Absatz 4 vorgeschlagene Änderung). Zu den bisherigen Erfahrungen mit der Zusammenarbeit gehört die auf Initiative der Kommission getroffene Vereinbarung, ein gemeinsames Verfahren für die Behandlung von grenzüberschreitenden Beschwerden über Spam einzuführen.

([1]) Stellungnahme des Europäischen Datenschutzbeauftragten zu der Mitteilung der Kommission an das Europäische Parlament und an den Rat zum Stand des Arbeitsprogramms für eine bessere Durchführung der Datenschutzrichtlinie (ABl. C 255 vom 27.10.2007, S. 1).

([2]) Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

63. Der EDSB ist der Ansicht, dass das Bestehen von Rechtsvorschriften, in denen die Unterstützung der Regulierungsbehörden durch die Regulierungsbehörden anderer Ländern geregelt wird, die grenzüberschreitende Durchsetzung zweifellos begünstigen wird. Deshalb sollte der Vorschlag die Kommission in die Lage versetzen, die Bedingungen für die Sicherstellung der grenzüberschreitenden Zusammenarbeit, einschließlich Verfahren für den Informationsaustausch, zu schaffen.

III. **FAZIT UND EMPFEHLUNGEN**

64. Der EDSB unterstützt den Vorschlag uneingeschränkt. Durch die vorgeschlagenen Änderungen wird der Schutz von Privatsphäre und personenbezogenen Daten in der elektronischen Kommunikation verbessert, und zwar durch maßvolle Änderungen, ohne einen ungerechtfertigten und unnötigen Verwaltungsaufwand zu verursachen. Insbesondere sollte nach Auffassung des EDSB der größte Teil der vorgeschlagenen Änderungen unverändert übernommen werden, da durch sie das angestrebte Ziel auf geeignete Weise erreicht werden kann. In Nummer 69 werden die Änderungsvorschläge aufgeführt, die nach Meinung des EDSB unverändert übernommen werden sollten.

65. Der EDSB kommt zwar in Bezug auf den Vorschlag zu einem insgesamt positiven Urteil, ist jedoch der Auffassung, dass einige der darin enthaltenen Änderungsvorschläge noch verbessert werden sollten, um sicherzustellen, dass durch sie die personenbezogenen Daten und die Privatsphäre des Einzelnen tatsächlich wirksam geschützt werden können. Verbessert werden sollten insbesondere die Bestimmungen zur Meldung von Sicherheitsverletzungen und die Bestimmungen zu den rechtlichen Schritten, die im Falle von Verstößen gegen die Spam-Vorschriften von einem Betreiber elektronischer Kommunikationsdienste ergriffen werden können. Darüber hinaus bedauert der EDSB, dass in dem Vorschlag auf einige Aspekte, die schon in der Datenschutzrichtlinie für die elektronische Kommunikation nicht gründlich behandelt wurden, gar nicht eingegangen wird und so bei dieser Überarbeitung die Gelegenheit verpasst wird, die bestehenden Probleme zu lösen.

66. Die Stellungnahme des EDSB enthält einige Textvorschläge, um bei beiden Problemen (d. h. im Vorschlag unzureichend oder aber gar nicht behandelte Aspekte) zu Lösungen zu gelangen. Die Nummern 67 und 68 enthalten eine zusammenfassende Darstellung der Probleme sowie spezifische Formulierungsvorschläge. Der Europäische Datenschutzbeauftragte ruft den Gesetzgeber auf, diese Vorschläge im weiteren Verlauf des Gesetzgebungsverfahrens zu berücksichtigen.

67. Unter anderem bei folgenden in dem Vorschlag enthaltenen Änderungsvorschlägen spricht sich der EDSB nachdrücklich für eine Überarbeitung aus:

i) **Meldung von Sicherheitsverletzungen:** In seinem derzeitigen Wortlaut gilt der Änderungsvorschlag, durch den *Artikel 4 Absatz 4* eingefügt wird, für Betreiber von öffentlich zugänglichen elektronischen Kommunikationsdiensten in öffentlichen Kommunikationsnetzen (Internet-Dienstanbieter, Netzbetreiber), die den nationalen Regulierungsbehörden und ihren Kunden Sicherheitsverletzungen melden müssen. Der EDSB befürwortet diese Verpflichtung voll und ganz, ist jedoch der Auffassung, dass sie ebenfalls für Betreiber von Diensten der Informationsgesellschaft gelten sollte, die oftmals sicherheitsempfindliche personenbezogene Daten verarbeiten. Dann würden auch On-line-Banken und On-line-Versicherungsunternehmen, On-line-Anbieter von Gesundheitsdiensten und jede andere Form von On-line-Unternehmen dieser Verpflichtung nachkommen müssen.

Der EDSB schlägt deshalb vor, in Artikel 4 Absatz 3 eine Bezugnahme auf die Betreiber von Diensten der Informationsgesellschaft wie folgt aufzunehmen: „*Im Falle einer Sicherheitsverletzung (…) muss der Betreiber der öffentlich zugänglichen elektronischen Kommunikationsdienste und der Betreiber der Dienste der Informationsgesellschaft den betroffenen Teilnehmer und die nationale Regulierungsbehörde (…) von der Sicherheitsverletzung benachrichtigen*“.

ii) **Rechtliche Schritte der Betreiber von öffentlich zugänglichen elektronischen Kommunikationsdienstes in öffentlichen Netzen:** In der aktuellen Fassung des Änderungsvorschlags, durch den *Artikel 13 Absatz 6* angefügt wird, ist vorgesehen, dass natürliche und juristische Personen und insbesondere die Anbieter elektronischer Kommunikationsdienste gerichtlich gegen Verstöße gegen Artikel 13 der Datenschutzrichtlinie für die elektronische Kommunikation, der unerbetene Nachrichten (Spam) zum Gegenstand hat, vorgehen können. Der EDSB unterstützt zwar diese Bestimmung, sieht jedoch keinen Grund dafür, diese neue Möglichkeit eines gerichtlichen Vorgehens auf Verstöße gegen Artikel 13 zu beschränken. Er schlägt vor, für juristische Personen die Möglichkeit zu schaffen, gerichtlich gegen Verstöße gegen jegliche Bestimmung der Richtlinie vorgehen zu können.

Deshalb schlägt er vor, Artikel 13 Absatz 6 in einen gesonderten Artikel (Artikel 14) umzuwandeln. Darüber hinaus sollte der Wortlaut des Artikels 13 Absatz 6 leicht abgewandelt werden: anstelle von „*aufgrund dieses Artikels*“ sollte es „aufgrund dieser Richtlinie“ heißen.

68. Der Anwendungsbereich der Datenschutzrichtlinie für die elektronische Kommunikation, der derzeit auf die Betreiber von öffentlichen elektronischen Kommunikationsnetzen beschränkt ist, ist eine der problematischsten Fragen, auf die in dem Vorschlag jedoch überhaupt nicht eingegangen wird. Nach Auffassung des EDSB sollte die Richtlinie dahingehend geändert werden, dass ihr Anwendungsbereich ausgeweitet wird, so dass auch die Betreiber elektronischer Kommunikationsdienste in gemischten (privaten/öffentlichen) und privaten Kommunikationsnetzen darunter fallen.

69. An folgenden Änderungen sollte nach Überzeugung des EDSB nicht gerührt werden:

i) **RFID:** Die vorgeschlagene Änderung von *Artikel 3*, wonach die elektronischen Kommunikationsnetze „*öffentliche Kommunikationsnetze, die Datenerfassungs- und Identifizierungsgeräte unterstützen*" einschließen, ist in vollem Umfang befriedigend. Diese Bestimmung ist sehr positiv zu sehen, da durch sie klargestellt wird, dass bei zahlreichen RFID-Anwendungen die Datenschutzrichtlinie für die elektronische Kommunikation eingehalten werden muss, womit eine gewisse Rechtsunsicherheit in dieser Hinsicht ausgeräumt wird.

ii) **Cookies/Spyware:** Die vorgeschlagene Änderung von *Artikel 5 Absatz 3* ist zu begrüßen, denn als Ergebnis hiervon wird die Verpflichtung zur Information und zur Einräumung eines Widerspruchs gegen die Speicherung von Cookies/Spyware in einem Endgerät auch dann gelten, wenn diese durch externe Datenspeichermedien wie CD-ROMs oder USB-Sticks eingeführt werden. Der EDSB befürwortet allerdings als geringfügige Änderung im letzten Satz von Artikel 5 Absatz 3 die Streichung der Worte „oder Erleichterung".

iii) **Wahl des Ausschussverfahrens mit Anhörung des EDSB und Bedingungen/Einschränkungen für die Meldepflicht:** Nach der vorgeschlagenen Änderung zur Aufnahme von Artikel 4 Absatz 4 betreffend die Meldung von Sicherheitsverletzungen sollen komplexe Fragen in Bezug auf Umstände/Form/Verfahren des Meldesystems bei Sicherheitsverletzungen nach Einholung der Stellungnahme des EDSB im Ausschussverfahren entschieden werden. Der EDSB befürwortet ganz entschieden diese einheitliche Vorgehensweise. Die Rechtsetzung für die Meldung von Sicherheitsverletzungen ist ein Thema, das eigenständig und nach gründlicher Erörterung und Analyse zu behandeln ist.

Verbunden mit dieser Frage ist der Wunsch bestimmter Akteure nach Ausnahmen von der Verpflichtung zur Meldung von Sicherheitsverletzungen nach Artikel 4 Absatz 4. Der EDSB lehnt dieses Ansinnen entschieden ab. Er ist eher für eine auf eine sachgerechte Erörterung folgende, ganzheitliche Analyse des Gesamtkomplexes der Meldung, d. h. wie die Benachrichtigung zu erfolgen hat, unter welchen Umständen sie verkürzt oder in irgendeiner Weise beschränkt werden kann.

iv) **Durchsetzung:** Die vorgeschlagene Änderung zur Aufnahme von *Artikel 15a* enthält viele hilfreiche und zu wahrende Elemente, die zur Gewährleistung einer effektiven Befolgung beitragen werden, wie die Stärkung der Untersuchungsbefugnisse der nationalen Regulierungsbehörden (Artikel 15a Absatz 3) und die Schaffung einer Befugnis für die nationalen Regulierungsbehörden, die Einstellung von Verstößen anzuordnen.

Brüssel, den 10. April 2008

Peter HUSTINX

Europäischer Datenschutzbeauftragter